S05P0372WO00

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001年7月19日 (19.07.2001)

PCT

(10) 国際公開番号
WO 01/52474 A1

(51) 国際特許分類[7]: H04L 9/32, 9/08, G06F 17/60

(21) 国際出願番号: PCT/JP01/00159

(22) 国際出願日: 2001年1月12日 (12.01.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-006989 2000年1月14日 (14.01.2000) JP
特願2000-041317 2000年2月18日 (18.02.2000) JP

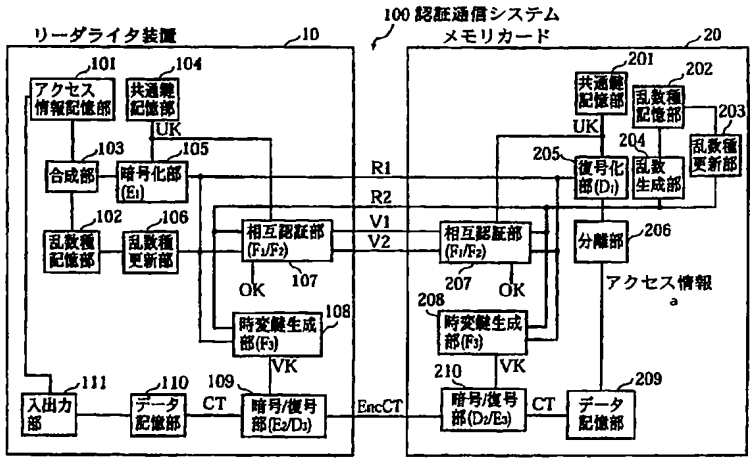
(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府門真市大字門真1006番地 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 柴田 修 (SHIBATA, Osamu) [JP/JP]; 〒570-0032 大阪府守口市菊水通1-16-22 Osaka (JP). 湯川泰平 (YUGAWA, Taihei) [JP/JP]; 〒631-0041 奈良県奈良市学園大和町6-708-1-513 Nara (JP). 関部 勉 (SEKIBE, Tsutomu) [JP/JP]; 〒573-0047 大阪府枚方市山之上5-49-34 Osaka (JP). 廣田照人 (HIROTA, Teruto) [JP/JP]; 〒570-0015 大阪府守口市梶町1-20-1-306 Osaka (JP). 齋藤義行 (SAITO, Yoshiyuki) [JP/JP]; 〒576-0053 大阪府交野市郡津1-1-611 Osaka (JP). 大竹俊彦 (OTAKE, Toshihiko)

[続葉有]

(54) Title: AUTHENTICATION COMMUNICATION DEVICE AND AUTHENTICATION COMMUNICATION SYSTEM

(54) 発明の名称: 認証通信装置及び認証通信システム




10...READER/WRITER
101...ACCESS INFORMATION STORAGE SECTION
104...COMMON KEY STORAGE SECTION
103...SYNTHESIZING SECTION
105...ENCRYPTING SECTION
102...RANDOM NUMBER TYPE STORAGE SECTION
106... RANDOM NUMBER TYPE UPDATING SECTION
107...MUTUAL AUTHENTICATING SECTION
108...TIME-VARYING KEY GENERATING SECTION
111...I/O SECTION
110...DATA STORAGE SECTION
109...ENCRYPTING/DECRYPTING SECTION
100...AUTHENTICATION COMMUNICATION SYSTEM
20...MEMORY CARD

201... COMMON KEY STORAGE SECTION
202...RANDOM NUMBER TYPE STORAGE SECTION
203... RANDOM NUMBER TYPE UPDATING SECTION
205... DECRYPTING SECTION
204...RANDOM NUMBER GENERATING SECTION
207... MUTUAL AUTHENTICATING SECTION
206...SEPARATING SECTION
208...TIME-VARYING KEY GENERATING SECTION
210...ENCRYPTING/DECRYPTING SECTION
209...DATA STORAGE SECTION
a...ACCESS INFORMATION

(57) Abstract: An authentication communication device comprises a storage medium having an area for storing digital information therein and an access unit for reading digital information from the area and writing digital information in the area. The access unit authenticates the storage medium according to a challenge response authentication protocol using disturbed access information produced by disturbing access information indicative of the area. The access unit is authenticated by the storage medium. When the validity is of both the storage medium and the access unit authenticated, the access unit reads out digital information from the area of the storage medium corresponding to access information separated from the disturbed access information or writes digital information therein.

[続葉有]

WO 01/52474 A1

[JP/JP]; 〒662-0095 兵庫県西宮市美作町5-12 Hyogo (JP).

(74) 代理人: 中島司朗(NAKAJIMA, Shiro); 〒531-0072 大阪府大阪市北区豊崎三丁目2番1号 淀川5番館6F Osaka (JP).

(81) 指定国 (国内): AU, CN, ID, KR, MX, US.

(84) 指定国 (広域): ヨーロッパ特許 (DE, FR, GB, NL).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

デジタル情報を記憶する領域を有する記憶媒体と、前記領域からデジタル情報を読み出し、又は前記領域へデジタル情報を書き込むアクセス装置とから構成され、前記アクセス装置において前記領域を示すアクセス情報を攪乱した攪乱化アクセス情報を用いたチャレンジレスポンス型認証プロトコルにより前記記憶媒体の認証を行うと共に、前記記憶媒体において、前記アクセス装置の認証を行い、共に正当性が認証された場合には、前記アクセス装置によって前記攪乱化アクセス情報から分離されたアクセス情報に応じた前記記憶媒体の前記領域にデジタル情報を読み出し、又は前記領域に書き込む。

# 明　細　書

## 認証通信装置及び認証通信システム

### 技術分野

本発明は、デジタル著作物を機器と記録媒体との間で転送する場合において、機器と記録媒体との間で、相互に正当性を認証する技術に関する。

### 背景技術

近年、デジタル情報圧縮技術の進展と、インターネットに代表されるグローバルな通信インフラの爆発的な普及によって、音楽、画像、映像、ゲームなどの著作物をデジタル著作物として通信回線を介して各家庭に配信することが実現されている。

デジタル著作物の著作権者の権利や、流通業者の利益を保護するための流通配信システムを確立するために、通信の傍受、盗聴、なりすましなどによる著作物の不正な入手や、受信したデータを記録している記録媒体からの違法な複製、違法な改竄などの不正行為を防止することが課題となっており、正規のシステムかどうかの判別を行ったり、データスクランブルを行う暗号及び認証などの著作物保護技術が必要とされている。

著作物保護技術については、従来より様々なものが知られており、代表的なものとして、著作物の保護を要する機密データが格納されている機密データ記憶領域にアクセスする際に、機器間で乱数と応答値の交換を行って、相互に正当性を認証しあい、正当である場合のみ、アクセスを許可するチャレンジレスポンス型の相互認証技術がある。

しかしながら、例えば、相互認証を正規な機器を用いて行った後に、正当機器になりすまして、機密データ記憶領域にアクセスすることによ

り、機密データを不正に入手する行為が考えられる。

発明の開示

そこで本発明はかかる問題点に鑑みてなされたものであり、機密データ記憶領域にアクセスするための情報が漏洩されないアクセス装置、記録媒体、認証通信システム、認証通信方法及び認証通信プログラムを記録している記録媒体を提供することを目的とする。

上記目的を達成するために本発明は、デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成される認証通信システムであって、前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第１認証フェーズと、前記記録媒体が前記アクセス装置の正当性の認証を行う第２認証フェーズと、前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送フェーズとを含むことを特徴とする。

これによって、相互認証と同時に、機密のデータを記録している機密データ記憶領域にアクセスするための情報を攪乱して転送するので、機密データ記憶領域にアクセスするための情報の機密性を高めることができる。

また、仮に、機密データ記憶領域にアクセスするための情報が、不正なりすましにより、別の情報に改竄されて転送された場合であっても、相互認証が成功しないので、機密データ記憶領域にアクセスできないようにすることができる。

図面の簡単な説明

図１は、認証通信システム１００の具体的な構成例としての認証通信システム３０及び３１の外観を示す。図１（ａ）は、パーソナルコンピュータとメモリカード２０から構成される認証通信システム３０の外観を示し、図１（ｂ）は、ヘッドホンステレオ、メモリカード２０及びヘッドホンから構成される認証通信システム３１の外観を示す。

図２は、認証通信システム１００を構成するリーダライタ装置１０及びメモリカード２０のそれぞれ構成を示すブロック図である。

図３は、アクセス情報、乱数種及び乱数化アクセス情報のデータ構造を示す。　図４は、認証通信システム１００の動作を示すフローチャートであり、特に、メモリカードに記憶されている情報を読み出す場合を想定したものである。図５に続く。

図５は、認証通信システム１００の動作を示すフローチャートである。図４から続く。

図６は、認証通信システム１００の動作を示すフローチャートであり、特に、リーダライタ装置１０は、メモリカードに情報を書き込む装置であると想定した場合のものである。

図７は、別の実施の形態としての、認証通信システム１００ａの構成を示すブロック図である。

図８は、認証通信システム１００ａに固有の動作を示すフローチャートである。

図９は、別の実施の形態としての、認証通信システム１００ｂの構成を示すブロック図である。

図１０は、認証通信システム１００ｂに固有の動作を示すフローチャートである。

発明を実施するための最良の形態

本発明に係る一つの実施の形態としての認証通信システム１００について説明する。

1．認証通信システム１００の外観と利用形態

認証通信システム１００の具体的な構成例としての認証通信システム３０及び３１の外観図を図１（ａ）及び（ｂ）に示す。

図１（ａ）に示すように、認証通信システム３０は、パーソナルコンピュータとメモリカード２０から構成される。パーソナルコンピュータは、ディスプレイ部、キーボード、スピーカ、マイクロプロセッサ、ＲＡＭ、ＲＯＭ、ハードディスクユニットなどを備えており、通信回線を経由してインターネットに代表されるネットワークに接続されている。メモリカード２０は、メモリカード挿入口から挿入され、パーソナルコンピュータに装着される。

図１（ｂ）に示すように、認証通信システム３１は、ヘッドホンステレオ、メモリカード２０及びヘッドホンから構成される。メモリカード２０は、ヘッドホンステレオのメモリカード挿入口から挿入されて、ヘッドホンステレオに装着される。ヘッドホンステレオは、上面に複数の操作ボタンが配置されており、別の側面にヘッドホンが接続されている。

利用者は、メモリカード２０をパーソナルコンピュータに装着し、インターネットを経由して、外部のＷｅｂサーバ装置から音楽などのデジタル著作物を取り込み、取り込んだデジタル著作物をメモリカード２０に書き込む。次に、利用者は、デジタル著作物の記録されているメモリカード２０をヘッドホンステレオに装着し、メモリカード２０に記録されているデジタル著作物をヘッドホンステレオにより再生して、楽しむ。

ここで、パーソナルコンピュータとメモリカード２０との間において、また、ヘッドホンステレオとメモリカード２０との間において、チャレンジレスポンス型の認証プロトコルによる各機器の正当性の認証を行い、相互に正当な機器であることが認証された場合にのみ、各機器間でデジタル著作物の転送が行われる。

2．認証通信システム１００の構成

認証通信システム１００は、図２に示すように、リーダライタ装置１

０及びメモリカード２０から構成される。ここで、リーダライタ装置１０は、図１（ａ）及び（ｂ）に示すパーソナルコンピュータ及びヘッドホンステレオに相当する。

２．１　リーダライタ装置１０の構成

リーダライタ装置１０は、アクセス情報記憶部１０１、乱数種記憶部１０２、合成部１０３、共通鍵記憶部１０４、暗号化部１０５、乱数種更新部１０６、相互認証部１０７、時変鍵生成部１０８、暗号復号部１０９、データ記憶部１１０及び入出力部１１１から構成されている。

リーダライタ装置１０は、具体的には、マイクロプロセッサ、ＲＡＭ、ＲＯＭその他を備え、ＲＯＭなどにコンピュータプログラムが記録されており、マイクロプロセッサは、前記コンピュータプログラムに従って動作する。

（１）入出力部１１１

入出力部１１１は、利用者の操作を受け付けて、メモリカード２０のデータ記憶部２０９に記憶されている音楽情報にアクセスするためのアクセス情報を生成する。アクセス情報は、図３に示すように、３２ビット長であり、メモリカード２０のデータ記憶部の領域のアドレスを示すアドレス情報と、前記領域のサイズを示すサイズ情報とから構成される。アドレス情報は、２４ビット長であり、サイズ情報は、８ビット長である。

また、入出力部１１１は、データ記憶部１１０から音楽情報ＣＴを読み出し、読み出した音楽情報ＣＴを音声信号に変換して出力する。

また、入出力部１１１は、利用者の操作を受け付けて、外部から音楽情報ＣＴを取得し、取得した音楽情報ＣＴをデータ記憶部１１０へ書き込む。

（２）アクセス情報記憶部１０１

アクセス情報記憶部１０１は、具体的には、半導体メモリから構成され、アクセス情報を記憶する領域を備えている。

（３）乱数種記憶部１０２

乱数種記憶部１０２は、具体的には、半導体メモリから構成され、図３に示すような６４ビット長の乱数種をあらかじめ記憶している。乱数種は、装置の製造時に記録される。

乱数種記憶部１０２は、外部から直接アクセスできる手段を有しておらず、プロテクトされている記憶手段である。

（４）合成部１０３

合成部１０３は、アクセス情報記憶部１０１からアクセス情報を読み出し、乱数種記憶部１０２から乱数種を読み出す。次に、図３に示すように、読み出した前記アクセス情報と、読み出した前記乱数種の下位３２ビットとを結合して、６４ビット長の乱数化アクセス情報を生成する。生成した乱数化アクセス情報を暗号化部１０５へ出力する。

（５）共通鍵記憶部１０４

共通鍵記憶部１０４は、具体的には、半導体メモリから構成され、５６ビット長の共通鍵ＵＫを記憶する領域を備えている。リーダライタ装置１０は、メモリカード２０から共通鍵記憶部２０１に記憶されている共通鍵ＵＫを秘密に取得し、共通鍵記憶部１０４は、取得した共通鍵ＵＫを記憶する。

共通鍵記憶部１０４は、外部から直接アクセスできる手段を有しておらず、プロテクトされている記憶手段である。

（６）暗号化部１０５

暗号化部１０５は、共通鍵記憶部１０４から共通鍵ＵＫを読み出し、合成部１０３から乱数化アクセス情報を受け取る。次に、暗号化部１０５は、共通鍵ＵＫを用いて、受け取った乱数化アクセス情報に暗号アルゴリズムＥ１を施して暗号化アクセス情報Ｒ１を生成する。ここで、暗号化部１０５は、暗号アルゴリズムＥ１として、ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）を用いる。

次に、暗号化部１０５は、生成した暗号化アクセス情報Ｒ１を、相互

認証部１０７と、乱数種更新部１０６と、時変鍵生成部１０８とへ出力する。また、生成した暗号化アクセス情報Ｒ１を、メモリカード２０の復号化部２０５と、相互認証部２０７と、時変鍵生成部２０８とへ出力する。

このようにして生成された暗号化アクセス情報Ｒ１は、アクセス情報に攪乱（ｓｃｒａｍｂｌｅ）処理を施して得られる攪乱化情報である。

（７）乱数種更新部１０６

乱数種更新部１０６は、暗号化部１０５から暗号化アクセス情報Ｒ１を受け取り、受け取った暗号化アクセス情報Ｒ１を新たな乱数種として乱数種記憶部１０２へ上書きする。

（８）相互認証部１０７

相互認証部１０７は、暗号化アクセス情報Ｒ１を受け取り、共通鍵記憶部１０４から共通鍵ＵＫを読み出し、受け取ったＲ１と共通鍵ＵＫとを用いて、式１により、応答値Ｖ２'を算出する。

（式１）　Ｖ２'＝Ｆ１（Ｒ１、ＵＫ）＝ＳＨＡ（Ｒ１＋ＵＫ）

ここで、関数Ｆ１（ａ、ｂ）は、一例として、ａとｂとを結合し、その結合結果に対してＳＨＡ（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ）を施す関数である。なお、＋は、結合を示す演算子である。

相互認証部１０７は、相互認証部２０７から応答値Ｖ２を受け取る。

次に、相互認証部１０７は、Ｖ２とＶ２'とが一致するか否かを判断し、一致しない場合には、メモリカード２０が不正な装置であると認定し、他の構成部に対して以降の動作の実行を禁止する。一致する場合には、相互認証部１０７は、メモリカード２０が正当な装置であると認定し、他の構成部に対して以降の動作の実行を許可する。

また、相互認証部１０７は、乱数生成部２０４から乱数Ｒ２を受け取り、受け取った乱数Ｒ２と、前記共通鍵ＵＫとを用いて、式２により、応答値Ｖ１を算出し、算出した応答値Ｖ１を相互認証部２０７へ出力する。

（式２）　Ｖ１＝Ｆ２（Ｒ２、ＵＫ）＝ＳＨＡ（Ｒ２＋ＵＫ）

（９）時変鍵生成部１０８

時変鍵生成部１０８は、メモリカード２０が正当な装置であると認定され、動作の実行を許可される場合に、暗号化アクセス情報Ｒ１と乱数Ｒ２とを受け取り、Ｒ１とＲ２とから、式３を用いて時変鍵ＶＫを生成する

（式３）　ＶＫ＝Ｆ３（Ｒ１、Ｒ２）＝ＳＨＡ（Ｒ１＋Ｒ２）

次に、時変鍵生成部１０８は、生成した時変鍵ＶＫを暗号復号部１０９へ出力する。

（１０）暗号復号部１０９

暗号復号部１０９は、時変鍵生成部１０８から時変鍵ＶＫを受け取る。

暗号復号部１０９は、暗号復号部２１０から暗号化音楽情報ＥｎｃＣＴを受け取り、前記時変鍵ＶＫを用いて、暗号化音楽情報ＥｎｃＣＴに復号アルゴリズムＤ３を施して音楽情報ＣＴを生成し、生成した音楽情報ＣＴをデータ記憶部１１０へ書き込む。

ここで、暗号復号部１０９は、復号アルゴリズムＥ３として、ＤＥＳを用いる。

また、暗号復号部１０９は、データ記憶部１１０から音楽情報ＣＴを読み出し、前記時変鍵ＶＫを用いて、音楽情報ＣＴに暗号アルゴリズムＥ２を施して暗号化音楽情報ＥｎｃＣＴを生成し、生成した暗号化音楽情報ＥｎｃＣＴを暗号復号部２１０へ出力する。

ここで、暗号復号部１０９は、暗号アルゴリズムＥ２として、ＤＥＳを用いる。

（１１）データ記憶部１１０

データ記憶部１１０は、具体的には、半導体メモリから構成され、音楽情報ＣＴを記憶する領域を備えている。

２．２　メモリカード２０

メモリカード２０は、共通鍵記憶部２０１、乱数種記憶部２０２、乱

数種更新部２０３、乱数生成部２０４、復号化部２０５、分離部２０６、相互認証部２０７、時変鍵生成部２０８、データ記憶部２０９及び暗号復号部２１０から構成されている。

（１）共通鍵記憶部２０１

共通鍵記憶部２０１は、具体的には、半導体メモリから構成され、５６ビット長の共通鍵ＵＫを記憶している。共通鍵ＵＫは、メモリカード２０の製造時に記録される。

共通鍵記憶部２０１は、外部から直接アクセスできる手段を有しておらず、プロテクトされている記憶手段である。

（２）乱数種記憶部２０２

乱数種記憶部２０２は、具体的には、半導体メモリから構成され、６４ビット長の乱数種をあらかじめ記憶している。乱数種は、メモリカード２０の製造時に記録される。

乱数種記憶部２０２は、外部から直接アクセスできる手段を有しておらず、プロテクトされている記憶手段である。

（３）乱数生成部２０４

乱数生成部２０４は、乱数種記憶部２０２から乱数種を読み出し、読み出した乱数種を用いて６４ビット長の乱数Ｒ２を生成し、生成した乱数Ｒ２を乱数種更新部２０３と、相互認証部２０７と、時変鍵生成部２０８とへ出力し、生成した乱数Ｒ２をリーダライタ装置１０の相互認証部１０７と、時変鍵生成部１０８とへ出力する。

（４）乱数種更新部２０３

乱数種更新部２０３は、乱数生成部２０４から乱数Ｒ２を受け取り、受け取った乱数Ｒ２を新たな乱数種として乱数種記憶部２０２へ上書きする。

（５）復号化部２０５

復号化部２０５は、共通鍵記憶部２０１から共通鍵ＵＫを読み出し、暗号化部１０５から暗号化アクセス情報Ｒ１を受け取る。次に、読み出

した共通鍵ＵＫを用いて、受け取った暗号化アクセス情報Ｒ１に、復号アルゴリズムＤ１を施して、乱数化アクセス情報を生成し、生成した乱数化アクセス情報を分離部２０６へ出力する。

ここで、復号化部２０５は、復号アルゴリズムＤ１として、ＤＥＳを用いる。復号アルゴリズムＤ１は、暗号アルゴリズムＥ１により生成された暗号文を復号する。

（６）分離部２０６

分離部２０６は、復号化部２０５から乱数化アクセス情報を受け取り、受け取った乱数化アクセス情報から、その上位３２ビットのデータをアクセス情報として分離し、アクセス情報をデータ記憶部２０９へ出力する。

（７）相互認証部２０７

相互認証部２０７は、共通鍵記憶部２０１から共通鍵ＵＫを読み出し、暗号化アクセス情報Ｒ１を受け取り、受け取ったＲ１と共通鍵ＵＫとを用いて、式４により、応答値Ｖ２を算出し、算出したＶ２をリーダライタ装置１０の相互認証部１０７へ出力する。

（式４）Ｖ２＝Ｆ１（Ｒ１、ＵＫ）＝ＳＨＡ（Ｒ１＋ＵＫ）

ここで、Ｆ１は、式１に示すＦ１と同じ関数であればよい。

また、相互認証部２０７は、乱数生成部２０４から乱数Ｒ２を受け取り、受け取った乱数Ｒ２と、前記共通鍵ＵＫとを用いて、式５により、応答値Ｖ１’を算出する。

（式５）Ｖ１’＝Ｆ２（Ｒ２、ＵＫ）＝ＳＨＡ（Ｒ２＋ＵＫ）

ここで、Ｆ２は、式２に示すＦ２と同じ関数であればよい。

次に、相互認証部２０７は、相互認証部１０７からＶ１を受け取り、Ｖ１とＶ１’とが一致するか否かを判断し、一致しない場合には、リーダライタ装置１０が不正な装置であると認定し、他の構成部に対して以降の動作の実行を禁止する。一致する場合には、相互認証部２０７は、リーダライタ装置１０が正当な装置であると認定し、他の構成部に対し

て以降の動作の実行を許可する。

（８）時変鍵生成部２０８

時変鍵生成部２０８は、リーダライタ装置１０が正当な装置であると認定され、動作の実行を許可される場合に、暗号化アクセス情報Ｒ１と乱数Ｒ２とを受け取り、Ｒ１とＲ２とから、式６を用いて時変鍵ＶＫを生成する

（式６）　ＶＫ＝Ｆ３（Ｒ１、Ｒ２）＝ＳＨＡ（Ｒ１＋Ｒ２）

ここで、Ｆ３は、式３に示す関数Ｆ３と同じである。

次に、時変鍵生成部２０８は、生成した時変鍵ＶＫを暗号復号部２１０へ出力する。

（９）データ記憶部２０９

データ記憶部２０９は、具体的には、半導体メモリから構成され、音楽情報ＣＴを記憶する領域を備えている。

（１０）暗号復号部２１０

暗号復号部２１０は、時変鍵生成部２０８から時変鍵ＶＫを受け取る。

暗号復号部２１０は、暗号復号部１０９から暗号化音楽情報ＥｎｃＣＴを受け取り、前記時変鍵ＶＫを用いて、暗号化音楽情報ＥｎｃＣＴに復号アルゴリズムＤ２を施して音楽情報ＣＴを生成し、生成した音楽情報ＣＴをデータ記憶部２０９の前記アクセス情報により示される領域へ書き込む。

ここで、暗号復号部２１０は、復号アルゴリズムＤ２として、ＤＥＳを用いる。復号アルゴリズムＤ２は、暗号アルゴリズムＥ２により生成された暗号文を復号する。

また、暗号復号部２１０は、データ記憶部２０９の前記アクセス情報により示される領域から音楽情報ＣＴを読み出し、前記時変鍵ＶＫを用いて、音楽情報ＣＴに暗号アルゴリズムＥ３を施して暗号化音楽情報ＥｎｃＣＴを生成し、生成した暗号化音楽情報ＥｎｃＣＴを暗号復号部１０９へ出力する。

ここで、暗号復号部２１０は、暗号アルゴリズムＥ３として、ＤＥＳを用いる。復号アルゴリズムＤ３は、暗号アルゴリズムＥ３により生成された暗号文を復号する。

３．認証通信システム１００の動作

（１）読み出し動作

認証通信システム１００を構成するリーダライタ装置１０及びメモリカード２０の動作について、図４～図５に示すフローチャートを用いて説明する。

なお、ここでは、リーダライタ装置１０は、図１（ｂ）に示すヘッドホンステレオのように、メモリカードに記憶されている情報を読み出す装置であると想定して説明する。

合成部１０３は、乱数種記憶部１０２から乱数種を読み出し、アクセス情報記憶部１０１からアクセス情報を読み出し、読み出した前記乱数種と読み出した前記アクセス情報とを合成して、乱数化アクセス情報を生成し（ステップＳ１０１）、暗号化部は、共通鍵記憶部１０４から共通鍵を読み出し、読み出した前記共通鍵を用いて乱数化アクセス情報を暗号化して暗号化アクセス情報Ｒ１を生成し（ステップＳ１０２）、相互認証部１０７は、Ｖ２′＝Ｆ１（Ｒ１）を算出し（ステップＳ１０３）、乱数種更新部１０６は、生成された乱数化アクセス情報を新たな乱数種として乱数種記憶部１０２に上書きする（ステップＳ１０４）。

暗号化部１０５は、生成した暗号化アクセス情報Ｒ１をメモリカード２０へ出力し、メモリカードの相互認証部２０７は、暗号化アクセス情報Ｒ１を受け取る（ステップＳ１０５）。

相互認証部２０７は、Ｖ２＝Ｆ１（Ｒ１）を算出し（ステップＳ１０６）、Ｖ２をリーダライタ装置１０の相互認証部１０７へ出力し、相互認証部１０７は、Ｖ２を受け取る（ステップＳ１０７）。

相互認証部１０７は、Ｖ２とＶ２′とが一致するか否かを判断し、一致しない場合には（ステップＳ１０８）、メモリカード２０が不正な装置

であると認定し、以後の動作を中止する。

一致する場合には（ステップＳ１０８）、相互認証部１０７は、メモリカード２０が正当な装置であると認定し、メモリカード２０の乱数生成部２０４は、乱数種記憶部２０２から乱数種を読み出し、読み出した乱数種を用いて乱数Ｒ２を生成し（ステップＳ１０９）、相互認証部２０７は、Ｖ１'＝Ｆ２（Ｒ２）を算出し（ステップＳ１１０）、乱数種更新部２０３は、生成された乱数Ｒ２を新たに乱数種として乱数種記憶部２０２に上書きする（ステップＳ１１１）。次に、乱数生成部２０４は、生成した乱数Ｒ２をリーダライタ装置１０の相互認証部１０７へ出力し、相互認証部１０７は、乱数Ｒ２を受け取り（ステップＳ１１２）、相互認証部１０７は、Ｖ１＝Ｆ２（Ｒ２）を生成し（ステップＳ１１３）、生成したＶ１をメモリカード２０の相互認証部２０７へ出力し、相互認証部２０７は、Ｖ１を受け取る（ステップＳ１１４）。

次に、相互認証部２０７

相互認証部２０７は、Ｖ１とＶ１'とが一致するか否かを判断し、一致しない場合には（ステップＳ１１５）、リーダライタ装置１０が不正な装置であると認定し、以後の動作を中止する。

一致する場合には（ステップＳ１１５）、相互認証部２０７は、リーダライタ装置１０が正当な装置であると認定し、リーダライタ装置１０の時変鍵生成部１０８は、Ｒ１とＲ２とを用いて時変鍵ＶＫを生成する（ステップＳ１２１）。メモリカード２０の復号化部２０５は、共通鍵記憶部２０１から共通鍵ＵＫを読み出し、読み出した共通鍵ＵＫを用いてＲ１を復号して乱数化アクセス情報を生成し（ステップＳ１２２）、分離部２０６は、乱数化アクセス情報からアクセス情報を分離し（ステップＳ１２３）、時変鍵生成部２０８は、Ｒ１とＲ２とを用いて時変鍵ＶＫを生成し（ステップＳ１２４）、暗号復号部２１０は、アクセス情報により示されるデータ記憶部２０９の領域から音楽情報ＣＴを読み出し（ステップＳ１２５）、暗号復号部２１０は、生成された時変鍵ＶＫを用いて読み出

した前記音楽情報ＣＴを暗号化して暗号化音楽情報ＥｎｃＣＴを生成し（ステップＳ１２６）、生成した暗号化音楽情報ＥｎｃＣＴをリーダライタ装置１０の暗号復号部１０９へ出力する（ステップＳ１２７）。

暗号復号部１０９は、時変鍵ＶＫを用いて暗号化音楽情報ＥｎｃＣＴを復号して音楽情報ＣＴを生成してデータ記憶部１１０へ書き込み（ステップＳ１２８）、入出力部１１１は、音楽情報ＣＴをデータ記憶部１１０から読み出し、読み出した音楽情報ＣＴを音声信号に変換して出力する（ステップＳ１２９）。

（２）書き込み動作

認証通信システム１００を構成するリーダライタ装置１０及びメモリカード２０の動作について、図６に示すフローチャートを用いて説明する。

ここでは、リーダライタ装置１０は、図１（ａ）に示すパーソナルコンピュータのように、メモリカードに情報を書き込む装置であると想定して説明する。また、読み出し動作と書き込み動作は類似しているので、相違点のみについて説明する。

図４～図５のフローチャートのステップＳ１２５～Ｓ１２９を、図６に示すステップに置き換えると認証通信システム１００の書き込み動作となる。

暗号復号部１０９は、データ記憶部１１０から音楽情報ＣＴを読み出し（ステップＳ１３１）、時変鍵ＶＫを用いて読み出した音楽情報ＣＴを暗号化して暗号化音楽情報ＣＴを生成し（ステップＳ１３２）、生成した暗号化音楽情報ＣＴをメモリカード２０の暗号復号部２１０へ出力し、暗号復号部２１０は、暗号化音楽情報ＣＴを受け取る（ステップＳ１３３）。

暗号復号部２１０は、暗号化音楽情報ＥｎｃＣＴを時変鍵ＶＫを用いて復号して音楽情報ＣＴを生成し（ステップＳ１３４）、生成した音楽情報ＣＴを前記アクセス情報で示されるデータ記憶部２０９内の領域に書

き込む（ステップＳ１３５）。

４．まとめ

以上説明したように、相互認証と同時に、機密のデータを記録している機密データ記憶領域にアクセスするための情報を攪乱して転送するので、機密データ記憶領域にアクセスするための情報の機密性を高めることができる。

また、仮に機密データ記憶領域にアクセスするための情報が、不正ななりすましにより、別の情報に改竄されて転送された場合であっても、相互認証が確立しないので、機密データ記憶領域にアクセスできないようにすることができる。

また、乱数の更新に機密データ記憶領域にアクセスするためのアクセス情報が関連していないので、乱数の周期性を高めることができる。

５．認証通信システム１００ａ

認証通信システム１００の変形例としての認証通信システム１００ａについて説明する。

５．１　認証通信システム１００ａの構成

認証通信システム１００ａは、図７に示すように、リーダライタ装置１０ａとメモリカード２０とから構成される。

メモリカード２０は、図２に示すメモリカード２０と同じであるので、ここでは、説明を省略する。

リーダライタ装置１０ａは、アクセス情報記憶部１０１、乱数種記憶部１０２、合成部１０３、共通鍵記憶部１０４、暗号化部１０５、乱数種更新部１０６、相互認証部１０７、時変鍵生成部１０８、暗号復号部１０９、データ記憶部１１０、入出力部１１１及び乱数生成部１１２から構成されている。

リーダライタ装置１０との相違点を中心として、以下に説明する。その他の点については、リーダライタ装置１０と同じであるので、説明を省略する。

（１）乱数生成部１１２

乱数生成部１１２は、乱数種記憶部１０２から乱数種を読み出し、読み出した乱数種を用いて６４ビット長の乱数を生成し、生成した乱数を合成部１０３と乱数種更新部１０６とへ出力する。

（２）乱数種更新部１０６

乱数種更新部１０６は、乱数生成部１１２から乱数を受け取り、受け取った乱数を新たな乱数種として乱数種記憶部１０２へ上書きする。

（３）合成部１０３

合成部１０３は、乱数生成部１１２から乱数を受け取り、アクセス情報記憶部１０１からアクセス情報を読み出し、受け取った前記乱数と読み出した前記アクセス情報とを合成して、乱数化アクセス情報を生成する。

５．２　認証通信システム１００ａの動作

認証通信システム１００ａの動作について、図８に示すフローチャートを用いて説明する。

乱数生成部１１２は、乱数種記憶部１０２から乱数種を読み出し（ステップＳ２０１）、読み出した乱数種を用いて６４ビット長の乱数を生成し（ステップＳ２０２）、乱数種更新部１０６は、乱数生成部１１２から乱数を受け取り、受け取った乱数を新たな乱数種として乱数種記憶部１０２へ上書きする（ステップＳ２０３）。次に、合成部１０３は、乱数生成部１１２から乱数を受け取り、アクセス情報記憶部１０１からアクセス情報を読み出し、受け取った前記乱数と読み出した前記アクセス情報とを合成して、乱数化アクセス情報を生成する（ステップＳ２０４）。

次に、図４のステップＳ１０２へ続く。以下は、認証通信システム１００の動作と同じであるので、説明を省略する。

５．３　まとめ

以上説明したように、乱数の更新に機密データ記憶領域にアクセスするためのアクセス情報が関連していないので、乱数の周期性を高めるこ

とができる。

６．認証通信システム１００ｂ

認証通信システム１００ａの変形例としての認証通信システム１００ｂについて説明する。

６．１　認証通信システム１００ｂの構成

認証通信システム１００ｂは、図９に示すように、リーダライタ装置１０ｂとメモリカード２０ｂとから構成される。

（１）リーダライタ装置１０ｂの構成

リーダライタ装置１０ｂは、アクセス情報記憶部１０１、乱数種記憶部１０２、合成部１０３、共通鍵記憶部１０４、暗号化部１０５、乱数種更新部１０６、相互認証部１０７、時変鍵生成部１０８、データ記憶部１１０、入出力部１１１、乱数生成部１１２、コンテンツ鍵生成部１１３、暗号化部１１４、コンテンツ付加情報記憶部１１５、暗号復号部１１６及び暗号化部１１７から構成されている。

以下において、リーダライタ装置１０ａとの相違点を中心として説明する。その他の点については、リーダライタ装置１０ａと同じであるので、説明を省略している。

（ａ）入出力部１１１

入出力部１１１は、利用者の操作によりコンテンツ付加情報の入力を受け付け、受け付けたコンテンツ付加情報をコンテンツ付加情報記憶部１１５に書き込む。

ここで、コンテンツ付加情報の一例は、コンテンツの再生回数、使用期間であり、コンテンツ付加情報は、８ビット長である。

また、入出力部１１１は、利用者の操作によりコンテンツデータＣＤを取得し、取得したコンテンツデータＣＤをデータ記憶部１１０に書き込む。

ここで、コンテンツデータＣＤは、一例として音楽コンテンツ情報である。

（ｂ）乱数生成部１１２

乱数生成部１１２は、生成した乱数Ｒ３をコンテンツ鍵生成部１１３へ出力する。

（ｃ）コンテンツ鍵生成部１１３

コンテンツ鍵生成部１１３は、コンテンツ付加情報記憶部１１５からコンテンツ付加情報を読み出し、乱数生成部１１２から乱数Ｒ３を受け取り、乱数Ｒ３と読み出したコンテンツ付加情報を用いて、式７により、コンテンツ鍵ＣＫを生成する。ここで、コンテンツ鍵ＣＫは、６４ビット長である。

（式７）ＣＫ＝Ｆ４（Ｒ３、コンテンツ付加情報）

＝コンテンツ付加情報（８ビット長）＋Ｒ３の下位５６ビット

ここで、＋は、データとデータの結合を示す演算子である。

次に、コンテンツ鍵生成部１１３は、生成したコンテンツ鍵ＣＫを暗号化部１１４と、暗号化部１１７とへ出力する。

（ｄ）暗号化部１１４

暗号化部１１４は、コンテンツ鍵生成部１１３からコンテンツ鍵ＣＫを受け取り、共通鍵記憶部１０４から共通鍵ＵＫを読み出し、読み出した共通鍵ＵＫを用いて、受け取ったコンテンツ鍵ＣＫに暗号化アルゴリズムＥ４を施して暗号化コンテンツ鍵ＥｎｃＣＫを生成し、生成した暗号化コンテンツ鍵ＥｎｃＣＫを暗号復号部１１６へ出力する。

ここで、暗号化部１１４は、暗号アルゴリズムＥ４として、ＤＥＳを用いる。（ｅ）暗号復号部１１６

暗号復号部１１６は、暗号化部１１４から暗号化コンテンツ鍵ＥｎｃＣＫを受け取り、受け取った暗号化コンテンツ鍵ＥｎｃＣＫに、時変鍵ＶＫを用いて、暗号アルゴリズムＥ２を施してＥｎｃ（ＥｎｃＣＫ）を生成し、生成したＥｎｃ（ＥｎｃＣＫ）を暗号復号部２１１へ出力する。

ここで、暗号復号部１１６は、暗号アルゴリズムＥ２として、ＤＥＳ

を用いる。

（ｆ）暗号化部１１７

暗号化部１１７は、データ記憶部１１０からコンテンツデータＣＤを読み出し、読み出したコンテンツデータＣＤに、コンテンツ鍵ＣＫを用いて、暗号化アルゴリズムＥ５を施して暗号化コンテンツデータＥｎｃＣＤを生成する。次に、暗号化部１１７は、生成した暗号化コンテンツデータＥｎｃＣＤをデータ記憶部２１３へ出力する。

ここで、暗号化部１１７は、暗号アルゴリズムＥ５として、ＤＥＳを用いる。

（２）メモリカード２０ｂの構成

メモリカード２０ｂは、共通鍵記憶部２０１、乱数種記憶部２０２、乱数種更新部２０３、乱数生成部２０４、復号化部２０５、分離部２０６、相互認証部２０７、時変鍵生成部２０８、暗号復号部２１１、鍵データ記憶部２１２及びデータ記憶部２１３から構成されている。

以下において、メモリカード２０との相違点を中心として説明する。その他の点については、メモリカード２０と同じであるので、説明を省略している。

（ａ）時変鍵生成部２０８

時変鍵生成部２０８は、時変鍵ＶＫを暗号復号部２１１へ出力する。

（ｂ）暗号復号部２１１

暗号復号部２１１は、時変鍵生成部２０８から時変鍵ＶＫを受け取り、暗号復号部１１６からＥｎｃ（ＥｎｃＣＫ）を受け取る。

次に、暗号復号部２１１は、時変鍵ＶＫを用いてＥｎｃ（ＥｎｃＣＫ）に復号アルゴリズムＤ２を施して暗号化コンテンツ鍵ＥｎｃＣＫを生成し、生成した暗号化コンテンツ鍵ＥｎｃＣＫを前記アクセス情報により示される鍵データ記憶部２１２の領域に書き込む。

（ｃ）鍵データ記憶部２１２

鍵データ記憶部２１２は、暗号化コンテンツ鍵ＥｎｃＣＫを記憶する

領域を備える。

（ｄ）データ記憶部２１３

データ記憶部２１３は、暗号化コンテンツデータＥｎｃＣＤを受け取り、受け取った暗号化コンテンツデータＥｎｃＣＤを記憶する。

６．２　認証通信システム１００ｂの動作

認証通信システム１００ｂの動作は、認証通信システム１００ａの動作に類似している。ここでは、認証通信システム１００ａとの相違点についてのみ説明する。

認証通信システム１００ｂの動作は、認証通信システム１００ａの動作を示すフローチャートのうち、ステップＳ１２１以降を図１０に示すフローチャートに置き換えたフローチャートにより示される。

コンテンツ鍵生成部１１３は、コンテンツ付加情報記憶部１１５からコンテンツ付加情報を読み出し（ステップＳ３０１）、乱数生成部１１２は、生成した乱数Ｒ３をコンテンツ鍵生成部１１３へ出力し、コンテンツ鍵生成部１１３は、乱数生成部１１２からＲ３を受け取り、Ｒ３と読み出したコンテンツ付加情報を用いて、コンテンツ鍵ＣＫを生成し、生成したコンテンツ鍵ＣＫを暗号化部１１４と、暗号化部１１７とへ出力し（ステップＳ３０２）、暗号化部１１４は、コンテンツ鍵生成部１１３からコンテンツ鍵ＣＫを受け取り、共通鍵記憶部１０４から共通鍵ＵＫを読み出し、読み出した共通鍵ＵＫを用いて、受け取ったコンテンツ鍵ＣＫに暗号化アルゴリズムＥ４を施して暗号化コンテンツ鍵ＥｎｃＣＫを生成し、生成した暗号化コンテンツ鍵ＥｎｃＣＫを暗号復号部１１６へ出力する（ステップＳ３０３）。次に、暗号復号部１１６は、暗号化コンテンツ鍵ＥｎｃＣＫを受け取り、受け取った暗号化コンテンツ鍵ＥｎｃＣＫに時変鍵ＶＫを用いて暗号アルゴリズムＥ２を施してＥｎｃ（ＥｎｃＣＫ）を生成し（ステップＳ３０４）、暗号復号部１１６は、生成したＥｎｃ（ＥｎｃＣＫ）を暗号復号部２１１へ出力し、暗号復号部２１１は、Ｅｎｃ（ＥｎｃＣＫ）を受け取り（ステップＳ３０５）、暗号復号

部２１１は、Ｅｎｃ（ＥｎｃＣＫ）に時変鍵ＶＫを用いて復号アルゴリズムＤ２を施して暗号化コンテンツ鍵ＥｎｃＣＫを生成し、生成した暗号化コンテンツ鍵ＥｎｃＣＫを前記アクセス情報により示される鍵データ記憶部２１２の領域に書き込む（ステップＳ３０６）。

暗号化部１１７は、データ記憶部１１０からコンテンツデータＣＤを読み出し（ステップＳ３０７）、読み出したコンテンツデータＣＤにコンテンツ鍵ＣＫを用いて暗号化アルゴリズムＥ５を施して暗号化コンテンツデータＥｎｃＣＤを生成する（ステップＳ３０８）。暗号化部１１７は、生成した暗号化コンテンツデータＥｎｃＣＤをデータ記憶部２１３へ出力し、データ記憶部２１３は、暗号化コンテンツデータＥｎｃＣＤを受け取り（ステップＳ３０９）、データ記憶部２１３は、受け取った暗号化コンテンツデータＥｎｃＣＤを記憶する（ステップＳ３１０）。

６．３　まとめ

以上説明したように、認証通信システム１００ｂにおいて、コンテンツデータを暗号化するためのコンテンツ鍵を生成するのに、新たな乱数発生機構を必要とぜず、アクセス情報の合成に用いる乱数発生機構と共有化できる。

７．その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

（１）上記の実施の形態において、デジタル著作物は、音楽の情報であるとしているが、小説や論文などの文字データ、コンピュータゲーム用のコンピュータプログラムソフトウェア、ＭＰ３などに代表される圧縮された音声データ、ＪＰＥＧなどの静止画像、ＭＰＥＧなどの動画像であるとしてもよい。

また、リーダライタ装置は、パーソナルコンピュータに限定されず、上記の様々なデジタル著作物を販売したり配布したりする出力装置であ

るとしてもよい。また、リーダライタ装置は、ヘッドホンステレオに限定されず、デジタル著作物を再生する再生装置であるとしてもよい。例えば、コンピュータゲーム装置、帯型情報端末、専用装置、パーソナルコンピュータなどであるとしてもよい。また、リーダライタ装置は、上記出力装置と再生装置との両方を兼ね備えているとしてもよい。

（２）上記の実施の形態において、暗号アルゴリズム及び復号アルゴリズムは、ＤＥＳを用いるとしているが、他の暗号を用いるとしてもよい。

また、上記実施の形態において、ＳＨＡを用いるとしているが、他の一方向性関数を用いるとしてもよい。

共通鍵、時変鍵の鍵長は、５６ビットであるとしているが、他の長さの鍵を用いるとしてもよい。

（３）上記の実施の形態において、合成部１０３は、アクセス情報と、乱数種の下位３２ビットとを結合して、６４ビット長の乱数化アクセス情報を生成するとしているが、これに限定されない。次のようにしてもよい。

合成部１０３は、３２ビットのアクセス情報と、乱数種の下位３２ビットとを１ビットずつ交互に結合して、６４ビット長の乱数化アクセス情報を生成していもよい。また、複数ビットずつ交互に結合してもよい。この場合、分離部２０６は、逆の操作を行うようにする。

（４）上記の実施の形態において、メモリカード２０の乱数生成部２０４は、乱数種記憶部２０２に記憶されている乱数種を用いて乱数Ｒ２を生成するとしているが、乱数生成部２０４は、乱数種を乱数Ｒ２として生成してもよい。

また、時変鍵生成部１０８、２０８は、Ｒ１及びＲ２を用いて時変鍵を生成するとしているが、応答値を用いるとしてもよい。また、共通鍵ＵＫを絡ませてもよい。

（５）認証通信システム１００ｂにおいて、暗号化部１１７は、暗号化コンテンツデータＥｎｃＣＤをデータ記憶部２１３に書き込むとしてい

るが、暗号化コンテンツデータＥｎｃＣＤを機密データとして扱って、アクセス情報により示される領域に書き込むとしてもよい。

また、暗号化コンテンツ鍵ＥｎｃＣＫを機密データとして扱わずに、データ記憶部２１３に書き込むとしてもよい。

また、暗号化部１１４及び暗号化部１１７のいずれか一方を無くし、残っている一方により共有化してもよい。

（６）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フロッピーディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

（４）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしても

よい。

産業上の利用の可能性

デジタル著作物を出力する出力装置から半導体記録媒体へデジタル著作物を複製する場合において、出力装置と半導体記録媒体とが、相互に正当性を認証する場合に利用することができる。また、デジタル著作物の記録されている半導体記録媒体からデジタル著作物を読み出して再生する場合において、半導体記録媒体と再生装置との間で、各装置が、相互に正当性を認証する場合に利用することができる。

# 請 求 の 範 囲

1．デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成される認証通信システムであって、

前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第1認証フェーズと、

前記記録媒体が前記アクセス装置の正当性の認証を行う第2認証フェーズと、

前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送フェーズと

を含むことを特徴とする認証通信システム。

2．前記第1認証フェーズにおいて、

前記アクセス装置は、

前記領域を示すアクセス情報を取得するアクセス情報取得部と、

乱数を取得する乱数取得部と、

取得した前記アクセス情報と、取得した乱数とを合成して乱数化アクセス情報を生成する生成部と、

生成した乱数化アクセス情報に暗号アルゴリズムを施して攪乱化アクセス情報を生成する暗号部とを含み、

前記記録媒体は、

生成された攪乱化アクセス情報から応答値を生成する応答値生成部とを含み、

前記アクセス装置は、

生成された前記応答値を用いて、前記記録媒体の正当性の認証を行う認証部を含む

ことを特徴とする請求の範囲１に記載の認証通信システム。

３．前記転送フェーズにおいて、

前記記録媒体は、

生成された攪乱化アクセス情報に復号アルゴリズムを施して乱数化アクセス情報を生成する復号部と、

伝送された乱数化アクセス情報からアクセス情報を分離する分離部とを含む

ことを特徴とする請求の範囲２に記載の認証通信システム。

４．前記第１認証フェーズにおいて、

前記アクセス装置は、さらに、乱数種を記憶している乱数種記憶部を含み、

前記乱数取得部は、乱数種記憶部から乱数種を読み出すことにより、乱数を取得する

ことを特徴とする請求の範囲３に記載の認証通信システム。

５．前記第１認証フェーズにおいて、

前記アクセス装置は、さらに、

前記攪乱化アクセス情報を乱数種として前記乱数種記憶部に上書きする

ことを特徴とする請求の範囲４に記載の認証通信システム。

６．前記第１認証フェーズにおいて、

前記アクセス装置は、さらに、乱数種を記憶している乱数種記憶部を含み、

前記乱数取得部は、乱数種記憶部から乱数種を読み出し、読み出した乱数種に基づいて乱数を生成することにより、乱数を取得する

ことを特徴とする請求の範囲３に記載の認証通信システム。

7．前記第１認証フェーズにおいて、

前記アクセス装置は、さらに、

生成された前記乱数を乱数種として前記乱数種記憶部に上書きする

ことを特徴とする請求の範囲６に記載の認証通信システム。

8．前記転送フェーズにおいて、

前記領域にデジタル情報を記録している記録媒体は、

前記アクセス情報により示される前記領域からデジタル情報を読み出し、読み出したデジタル情報に暗号アルゴリズムを施して暗号化デジタル情報を生成する暗号部を含み、

前記領域からデジタル情報を読み出す前記アクセス装置は、

生成された暗号化デジタル情報に復号アルゴリズムを施してデシタル情報を生成する復号部を含み、

前記復号アルゴリズムは、前記暗号アルゴリズムにより生成された暗号文を復号する

ことを特徴とする請求の範囲３に記載の認証通信システム。

9．前記転送フェーズにおいて、

前記領域へデジタル情報を書き込む前記アクセス装置は、

デジタル情報を取得するデジタル情報取得部と、

取得したデジタル情報に暗号アルゴリズムを施して暗号化デシタル情報を生成する暗号部を含み、

前記記録媒体は、

生成された前記暗号化デジタル情報に復号アルゴリズムを施してデジタル情報を生成し、前記アクセス情報により示される前記領域へデジタル情報を書き込む復号部を含み、

前記復号アルゴリズムは、前記暗号アルゴリズムにより生成された暗号文を復号する

ことを特徴とする請求の範囲３に記載の認証通信システム。

10．前記転送フェーズにおいて、

前記領域へデジタル情報を書き込む前記アクセス装置は、

デジタル情報を取得するデジタル情報取得部と、

コンテンツ鍵を取得するコンテンツ鍵取得部と、

取得したコンテンツ鍵に第１暗号アルゴリズムを施して暗号化コンテンツ鍵を生成する第１暗号部と、

生成された前記暗号化コンテンツ鍵に第２暗号アルゴリズムを施して二重暗号化コンテンツ鍵を生成する第２暗号化部と、

前記コンテンツ鍵を用いて、取得した前記デジタル情報に第２暗号アルゴリズムを施して暗号化デシタル情報を生成する第３暗号部とを含み、

前記記録媒体は、

生成された前記二重暗号化コンテンツ鍵に第１復号アルゴリズムを施して暗号化コンテンツ鍵を生成し、前記アクセス情報により示される前記領域へ暗号化コンテンツ鍵を書き込む復号部を含み、

前記記録媒体は、さらに、生成された前記暗号化デジタル情報を記憶する領域を含む

ことを特徴とする請求の範囲３に記載の認証通信システム。

11. デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成される認証通信システムで用いられる認証通信方法であって、

前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第１認証ステップと、

前記記録媒体が前記アクセス装置の正当性の認証を行う第２認証ステップと、

前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアク

セス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送ステップと

を含むことを特徴とする認証通信方法。

12. デジタル情報を記憶する領域を有する記録媒体と、前記領域からデジタル情報を読み出し又は前記領域へデジタル情報を書き込むアクセス装置とから構成され、前記記録媒体と前記アクセス装置との間において各機器の正当性の認証を行った後に、デジタル情報を転送する認証通信システムで用いられる認証通信プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、

前記認証通信プログラムは、

前記アクセス装置から前記記録媒体へ、前記領域を示すアクセス情報を攪乱して生成した攪乱化アクセス情報を伝送することにより、前記アクセス装置がチャレンジレスポンス型の認証プロトコルによる前記記録媒体の正当性の認証を行う第１認証ステップと、

前記記録媒体が前記アクセス装置の正当性の認証を行う第２認証ステップと、

前記記録媒体と前記アクセス装置とがともに正当性を有すると認証された場合に、前記記録媒体は、伝送された攪乱化アクセス情報からアクセス情報を抽出し、前記アクセス装置は、抽出された前記アクセス情報により示される領域からデジタル情報を読み出し、又は前記アクセス情報により示される領域へデジタル情報を書き込む転送ステップと

を含むことを特徴とする記録媒体。

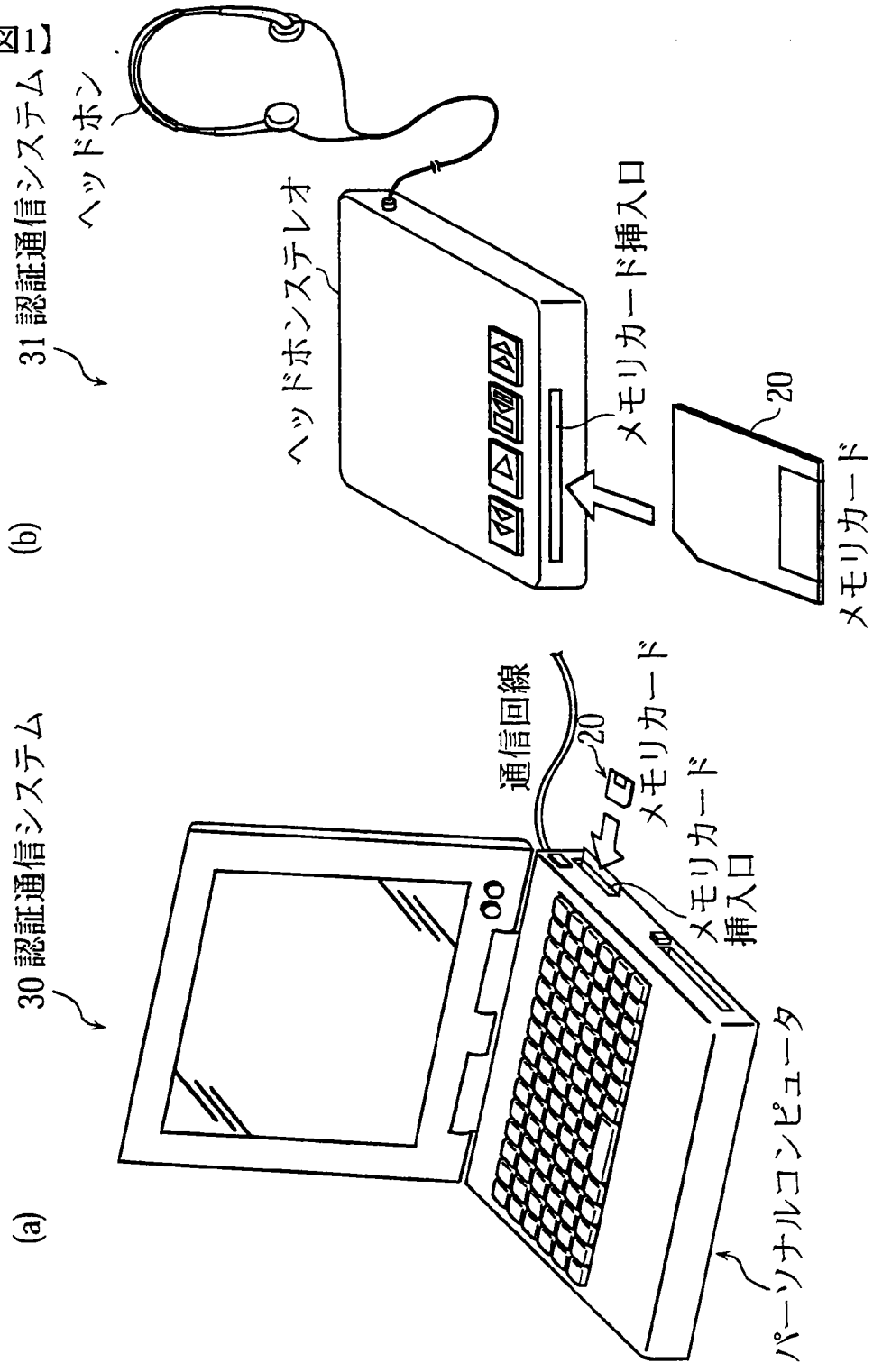
13. 請求の範囲１に記載の認証通信システムを構成するアクセス装置。

14. 請求の範囲２に記載の認証通信システムを構成するアクセス装置。

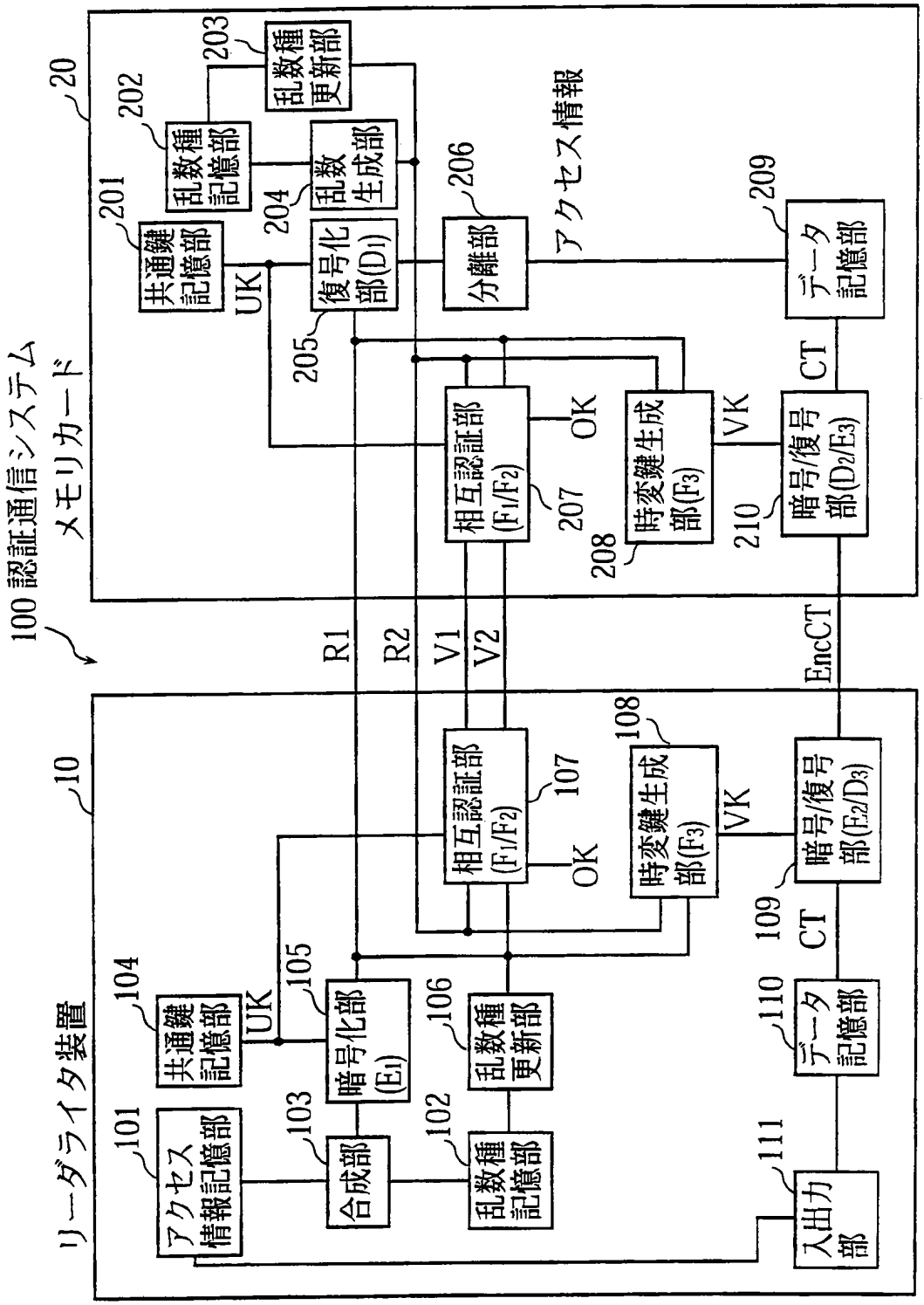
15. 請求の範囲１に記載の認証通信システムを構成する記録媒体。

16. 請求の範囲３に記載の認証通信システムを構成する記録媒体。

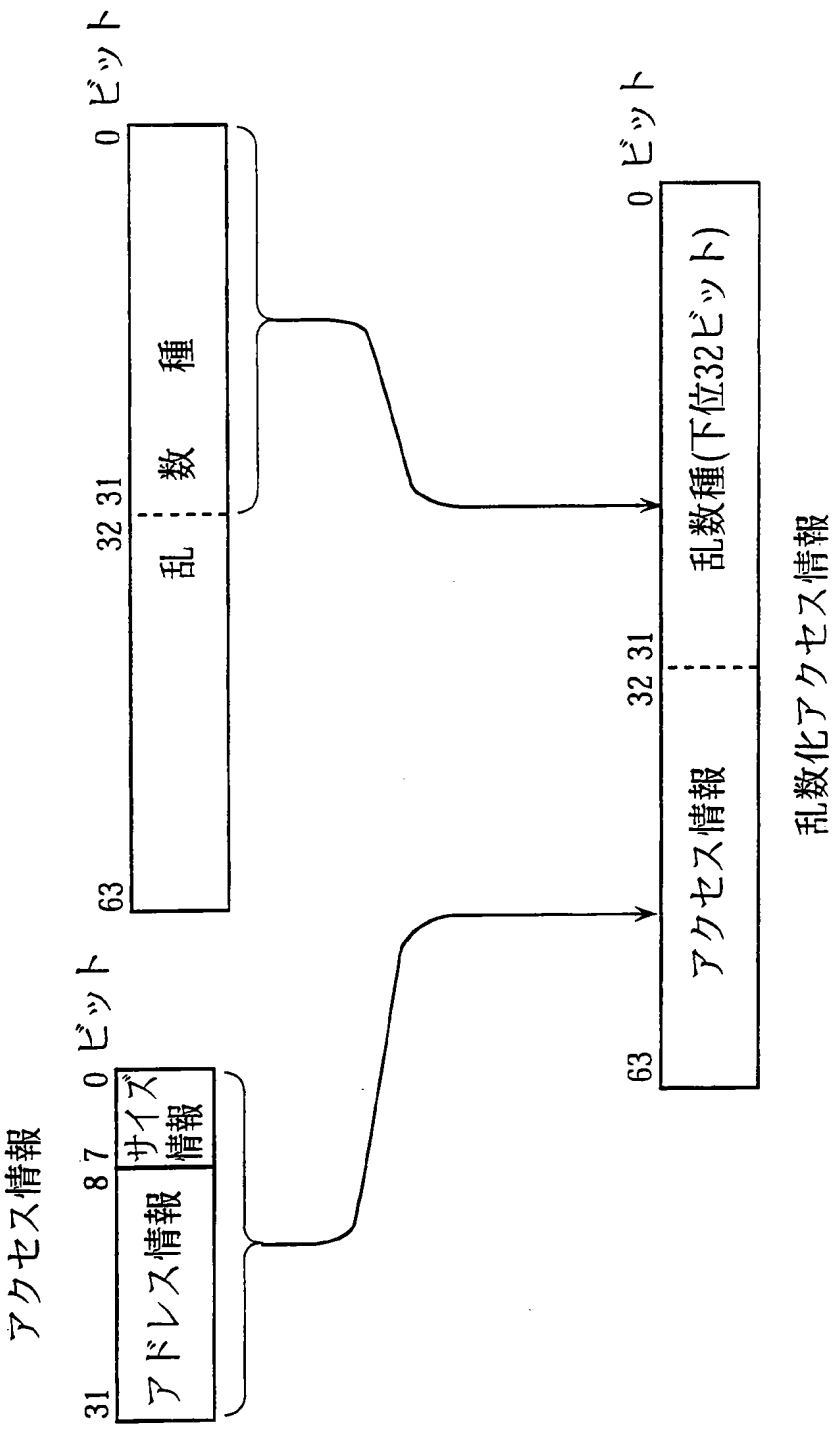
【図1】


(a)
30 認証通信システム
パーソナルコンピュータ
メモリカード
挿入口
メモリカード
20
通信回線
(b)
31 認証通信システム
ヘッドホン
ヘッドホンステレオ
メモリカード挿入口
メモリカード
20

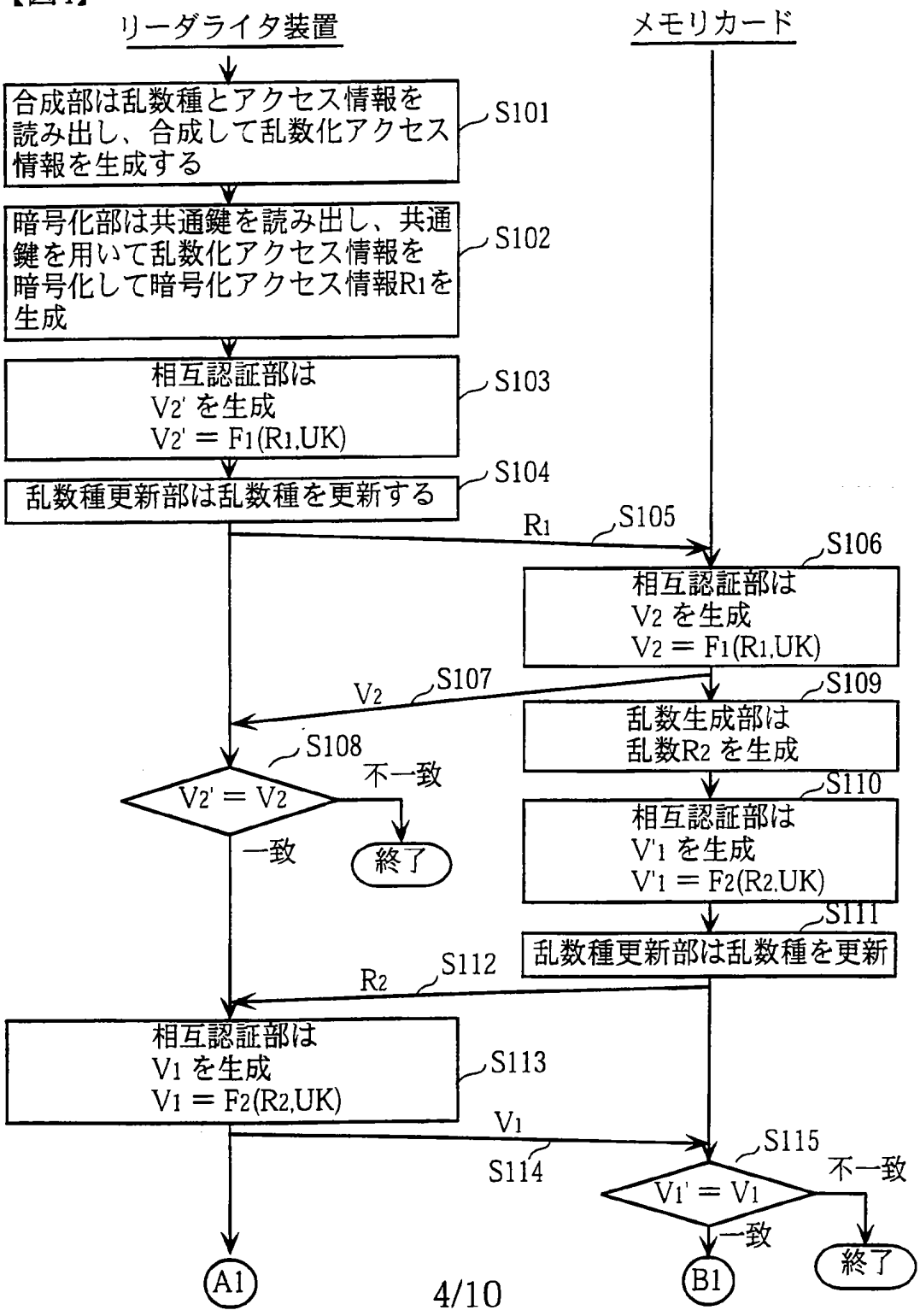
【図2】


100 認証通信システム
メモリカード
20
201 共通鍵記憶部
202 乱数種記憶部
203 乱数種更新部
204 乱数生成部
205 復号化部(D1)
206 分離部
209 データ記憶部
相互認証部(F1/F2)
207
OK
時変鍵生成部(F3)
208
VK
210 暗号/復号部(D2/E3)
CT
UK
アクセス情報
R1
R2
V1
V2
EncCT
リーダライタ装置
10
104 共通鍵記憶部
105 暗号化部(E1)
106 乱数種更新部
107
108 時変鍵生成部(F3)
109
暗号/復号部(F2/D3)
110 データ記憶部
111 入出力部
101 アクセス情報記憶部
103 合成部
102 乱数種記憶部

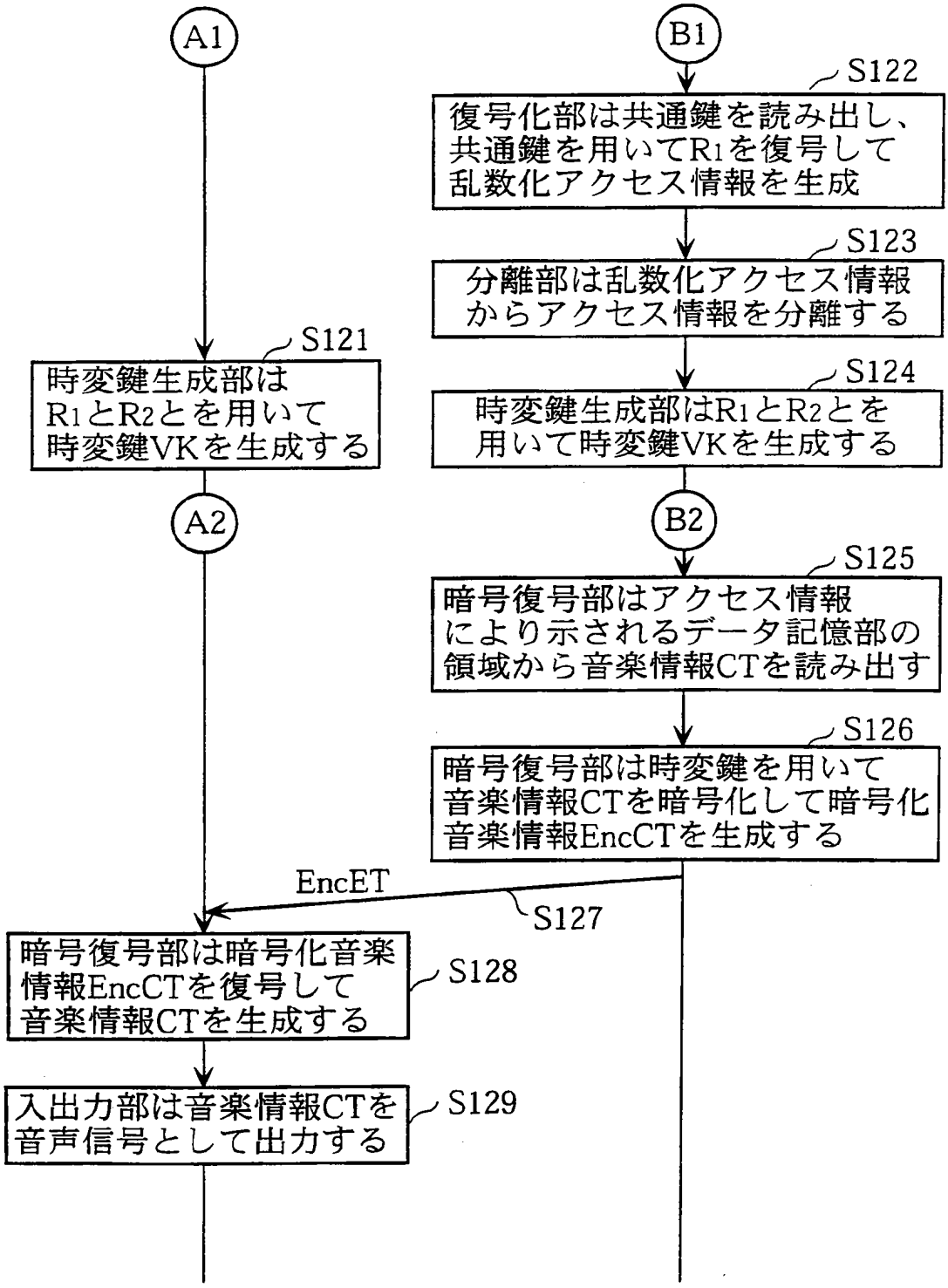
【図3】


アクセス情報
0 ビット
31
アドレス情報
8 7
0
サイズ情報
0 ビット
63
乱数種
32 31
乱数化アクセス情報
0 ビット
63
アクセス情報
32 31
乱数種(下位32ビット)

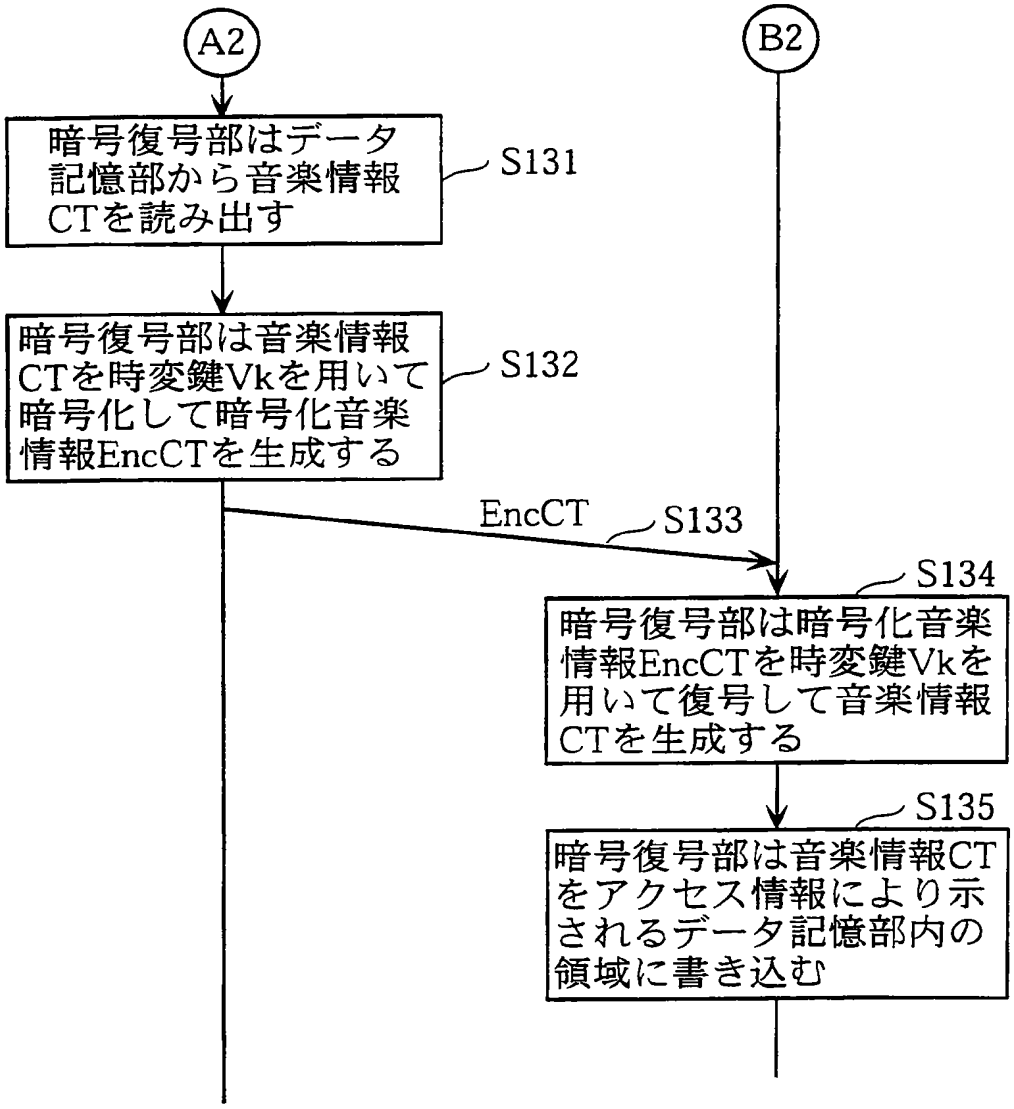
【図4】


リーダライタ装置
メモリカード
合成部は乱数種とアクセス情報を読み出し、合成して乱数化アクセス情報を生成する
S101
暗号化部は共通鍵を読み出し、共通鍵を用いて乱数化アクセス情報を暗号化して暗号化アクセス情報R1を生成
S102
相互認証部は
V2' を生成
V2' = F1(R1,UK)
S103
乱数種更新部は乱数種を更新する
S104
R1
S105
S106
相互認証部は
V2 を生成
V2 = F1(R1,UK)
V2
S107
S109
乱数生成部は
乱数R2 を生成
S108
V2' = V2
不一致
一致
終了
S110
相互認証部は
V'1 を生成
V'1 = F2(R2,UK)
S111
乱数種更新部は乱数種を更新
R2
S112
相互認証部は
V1 を生成
V1 = F2(R2,UK)
S113
V1
S114
S115
V1' = V1
不一致
一致
終了
A1
B1

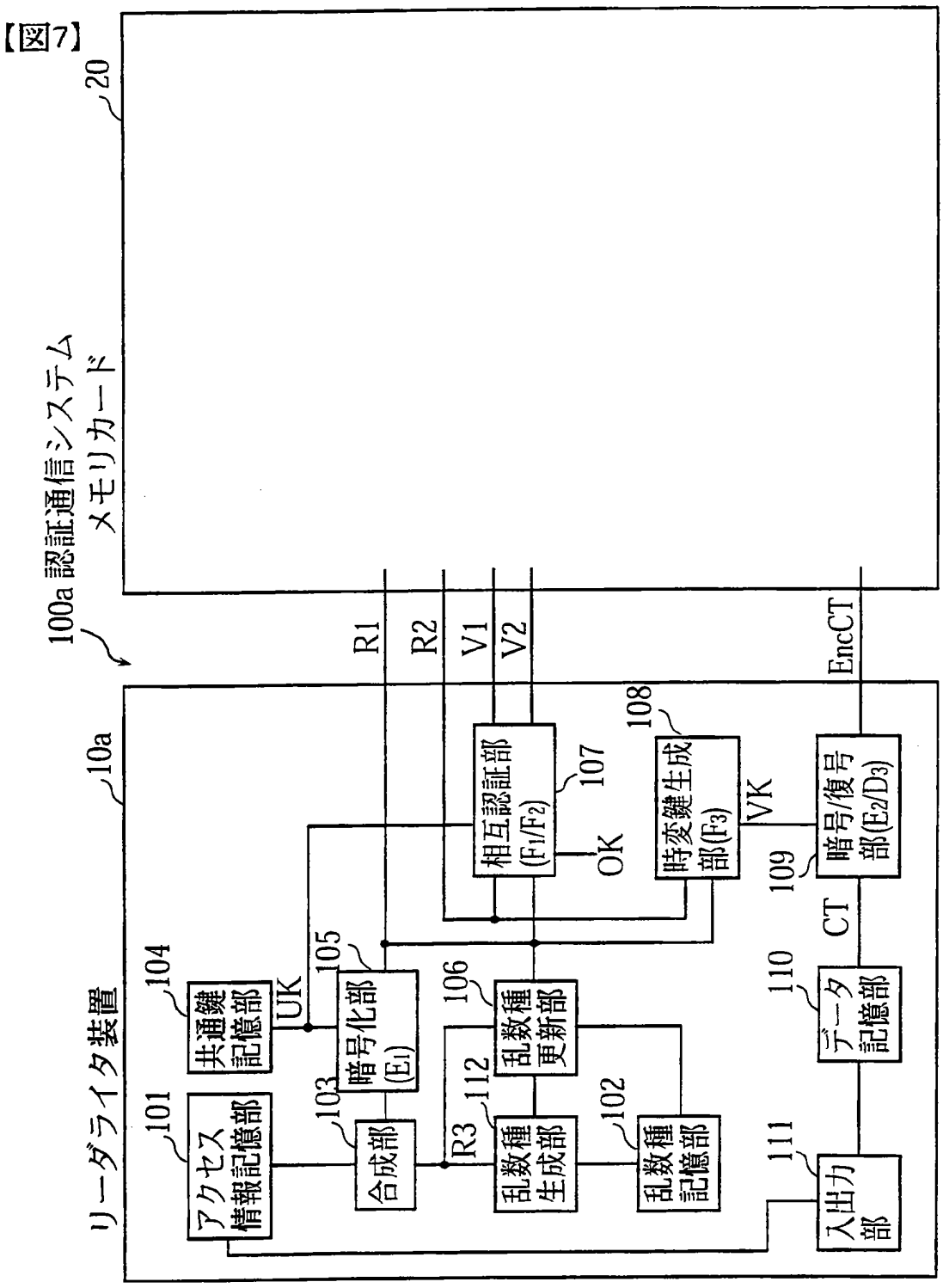
【図5】


A1
B1
S122
復号化部は共通鍵を読み出し、共通鍵を用いてR1を復号して乱数化アクセス情報を生成
S123
分離部は乱数化アクセス情報からアクセス情報を分離する
S121
時変鍵生成部はR1とR2とを用いて時変鍵VKを生成する
S124
時変鍵生成部はR1とR2とを用いて時変鍵VKを生成する
A2
B2
S125
暗号復号部はアクセス情報により示されるデータ記憶部の領域から音楽情報CTを読み出す
S126
暗号復号部は時変鍵を用いて音楽情報CTを暗号化して暗号化音楽情報EncCTを生成する
EncET
S127
暗号復号部は暗号化音楽情報EncCTを復号して音楽情報CTを生成する
S128
入出力部は音楽情報CTを音声信号として出力する
S129

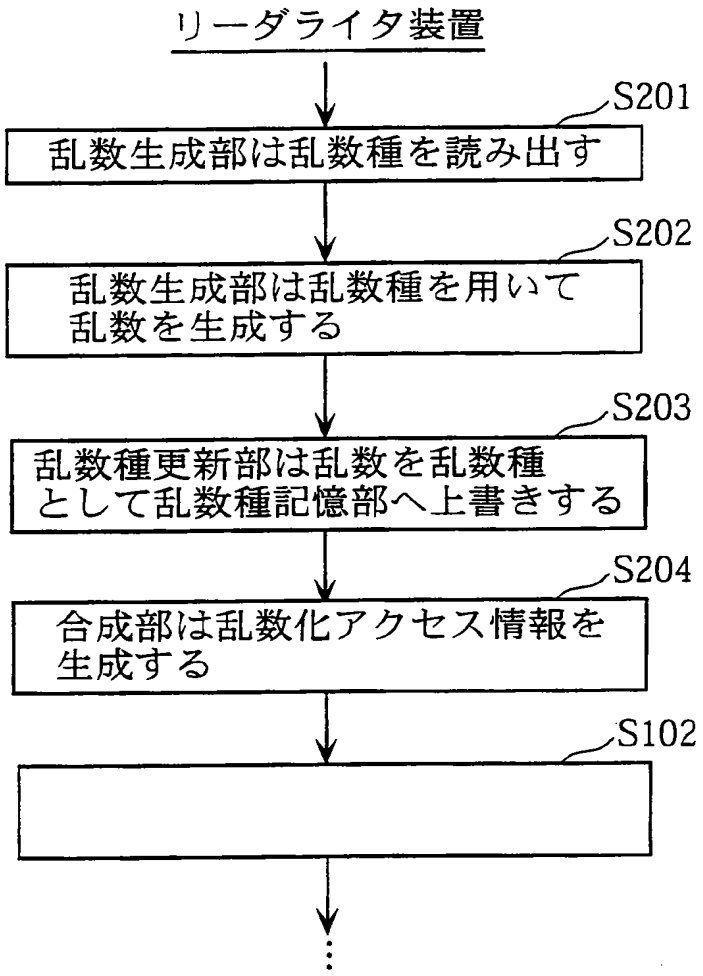
【図6】


A2
B2
暗号復号部はデータ記憶部から音楽情報CTを読み出す
S131
暗号復号部は音楽情報CTを時変鍵Vkを用いて暗号化して暗号化音楽情報EncCTを生成する
S132
EncCT
S133
S134
暗号復号部は暗号化音楽情報EncCTを時変鍵Vkを用いて復号して音楽情報CTを生成する
S135
暗号復号部は音楽情報CTをアクセス情報により示されるデータ記憶部内の領域に書き込む

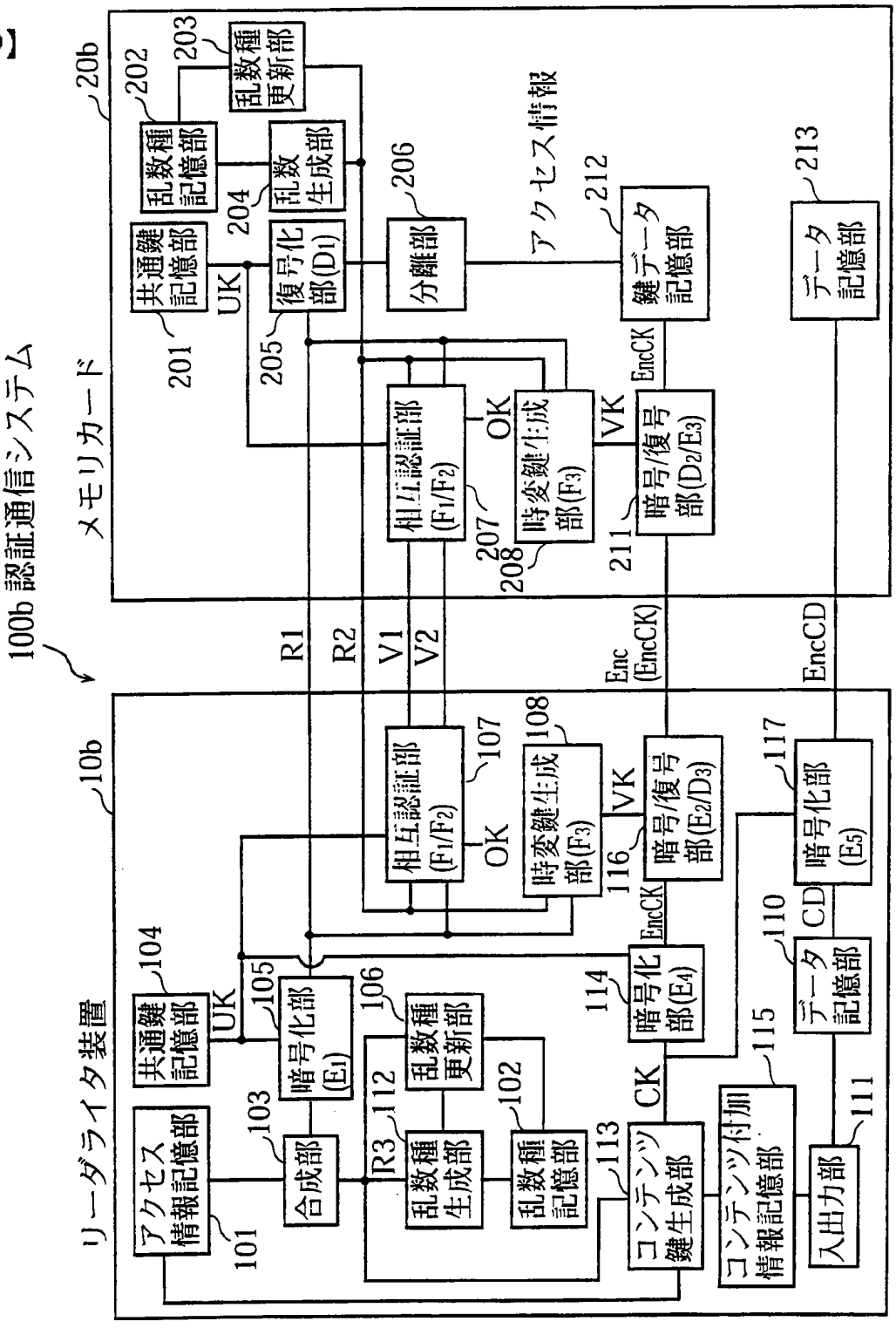
【図7】


100a 認証通信システム
メモリカード
20
リーダライタ装置
10a
R1
R2
V1
V2
EncCT
アクセス情報記憶部
101
共通鍵記憶部
104
UK
暗号化部 (E1)
105
合成部
103
乱数種生成部
112
R3
乱数種更新部
106
乱数種記憶部
102
相互認証部 (F1/F2)
107
OK
時変鍵生成部(F3)
108
VK
暗号/復号部(E2/D3)
109
CT
データ記憶部
110
入出力部
111

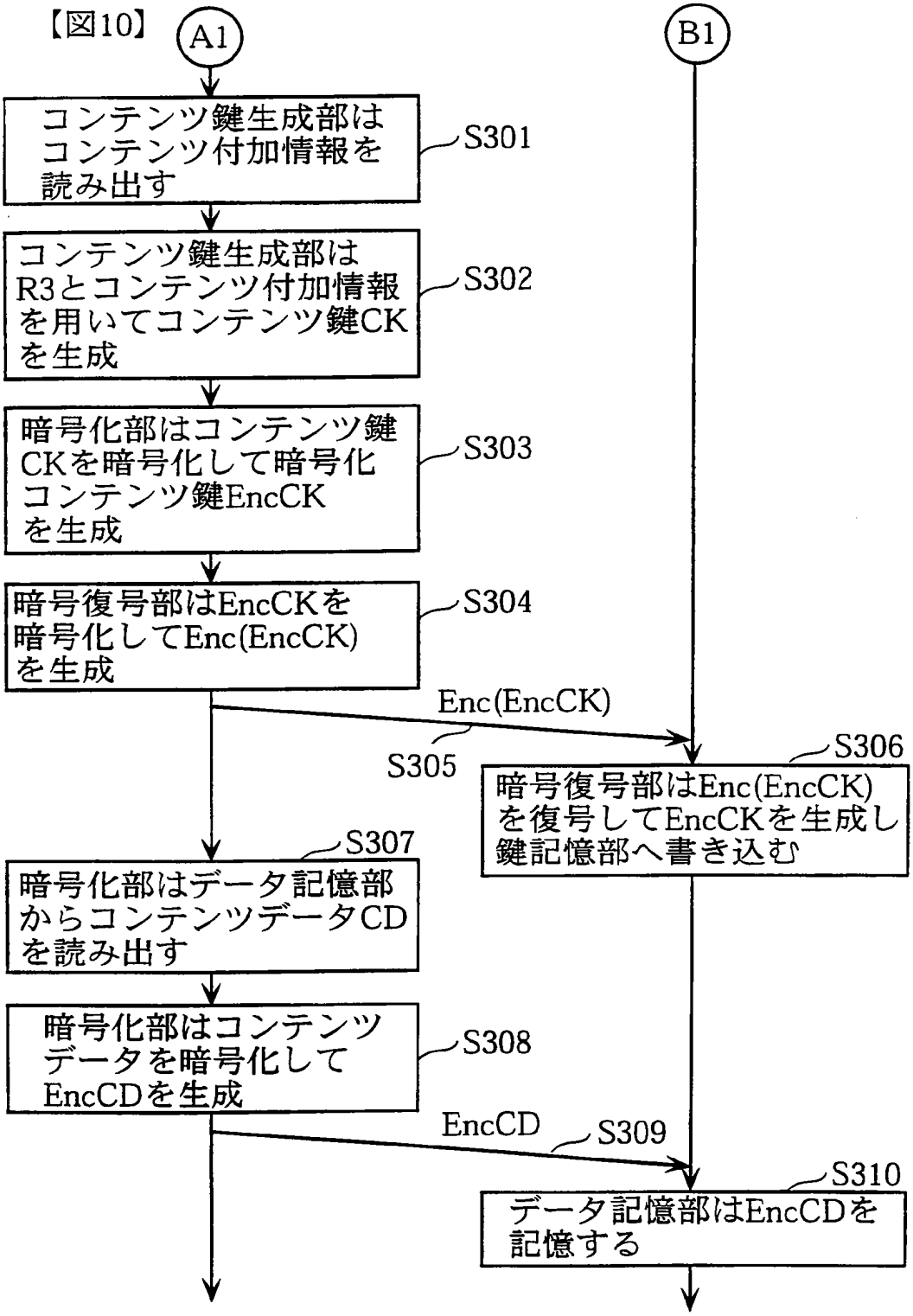
【図8】


リーダライタ装置
S201
乱数生成部は乱数種を読み出す
S202
乱数生成部は乱数種を用いて乱数を生成する
S203
乱数種更新部は乱数を乱数種として乱数種記憶部へ上書きする
S204
合成部は乱数化アクセス情報を生成する
S102

【図9】


100b 認証通信システム
リーダライタ装置
10b
メモリカード
20b
アクセス情報記憶部
101
合成部
103
暗号化部(E1)
105
共通鍵記憶部
104
UK
乱数種更新部
106
乱数種生成部
112
乱数種記憶部
102
113
コンテンツ鍵生成部
CK
コンテンツ付加情報記憶部
115
入出力部
111
暗号化部(E4)
114
EncCK
相互認証部(F1/F2)
107
OK
時変鍵生成部(F3)
108
VK
暗号/復号部(E2/D3)
116
Enc(EncCK)
データ記憶部
110
CD
暗号化部(E5)
117
EncCD
R1
R2
V1
V2
R3
共通鍵記憶部
201
UK
乱数種記憶部
202
乱数種更新部
203
乱数生成部
204
復号化部(D1)
205
分離部
206
相互認証部(F1/F2)
207
OK
時変鍵生成部(F3)
208
VK
暗号/復号部(D2/E3)
211
EncCK
鍵データ記憶部
212
データ記憶部
213

【図10】


A1
B1
コンテンツ鍵生成部はコンテンツ付加情報を読み出す
S301
コンテンツ鍵生成部はR3とコンテンツ付加情報を用いてコンテンツ鍵CKを生成
S302
暗号化部はコンテンツ鍵CKを暗号化して暗号化コンテンツ鍵EncCKを生成
S303
暗号復号部はEncCKを暗号化してEnc(EncCK)を生成
S304
Enc(EncCK)
S305
S306
暗号復号部はEnc(EncCK)を復号してEncCKを生成し鍵記憶部へ書き込む
S307
暗号化部はデータ記憶部からコンテンツデータCDを読み出す
暗号化部はコンテンツデータを暗号化してEncCDを生成
S308
EncCD
S309
S310
データ記憶部はEncCDを記憶する